

NAVAL POSTGRADUATE SCHOOL Monterey, California



Research Opportunities in Joint Interoperability Testing

by

Robert A. Koyak

September 1999

Approved for public release; distribution is unlimited.

Prepared for: Defense Information Systems Agency
Joint Interoperability Test Command
Fort Huachuca, AZ 85613-7020

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA 93943-5000


RADM Robert C. Chaplin
Superintendent

Richard Elster
Provost

This report was prepared for and funded by the Defense Information Systems Agency,
Joint Interoperability Test Command, Fort Huachuca, AZ 85613-7020.

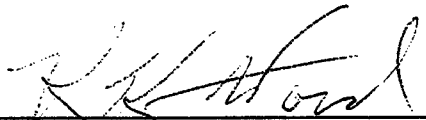
Reproduction of all or part of this report is authorized.

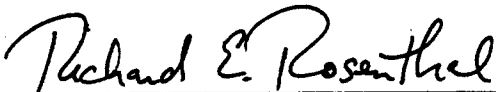
This report was prepared by:



ROBERT A. KOYAK
Assistant Professor of
Operations Research

Reviewed by:

Released by:


R. KEVIN WOOD
Associate Chairman for Research
Department of Operations Research


RICHARD E. ROSENTHAL
Chairman
Department of Operations Research


DAVID W. NETZER
Associate Provost and Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

September 1999

3. REPORT TYPE AND DATES COVERED

Technical

4. TITLE AND SUBTITLE

Research Opportunities in Joint Interoperability Testing

5. FUNDING

MIPRJITCMH4199

6. AUTHOR(S)

Robert A. Koyak

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 939438. PERFORMING ORGANIZATION
REPORT NUMBER

NPS-OR-99-006

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Information Systems Agency
Joint Interoperability Test Command
Attn: Deputy Commander Denis Beaugureau
Fort Huachuca, AZ 85613-702010. SPONSORING/MONITORING
AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The Department of Defense requires that all command, control, communications and computers intelligence (C4I) systems and automated information systems (AIS) be interoperable between the services. The Joint Interoperability Test Command (JITC) is responsible for testing and certifying the joint interoperability of these systems. The design of joint interoperability tests and the analysis of data that they produce offer many opportunities for NPS faculty and students to collaborate with JITC on research projects of mutual interest. This paper outlines a spectrum of potential research opportunities, encompassing probability and statistics, modeling and simulation, computer science, information technology, electrical engineering, human factors, and specialized subject matter related to intelligence, communications, and missile defense systems.

14. SUBJECT TERMS

joint interoperability testing, testing and evaluation, collaborative research

15. NUMBER OF
PAGES

34

16. PRICE CODE

17. SECURITY CLASSIFICATION
OF REPORT

Unclassified

18. SECURITY CLASSIFICATION
OF THIS PAGE

Unclassified

19. SECURITY CLASSIFICATION
OF ABSTRACT

Unclassified

20. LIMITATION OF
ABSTRACT

UL

Executive Summary

The Department of Defense requires that all command, control, communications and computers intelligence (C4I) systems and automated information systems (AIS) be interoperable between the services. The Joint Interoperability Test Command (JITC), located at Fort Huachuca, AZ, is responsible for testing and certifying the joint interoperability of these systems. Joint interoperability testing shares many of the general features of operational testing and evaluation, but it also has features that are unique in concept. A C4I or AIS system may be fully operational, yet fail to handshake properly with related applications when configured together in a network. It is well recognized that a failure of C4I or AIS systems to interoperate can have serious consequences for military operations.

The purpose of this paper is to describe a range of activities in which the faculty and students of the Naval Postgraduate School (NPS) may find opportunities to collaborate with JITC on the design and analysis of joint interoperability testing. This paper is the culmination of a study that the author conducted at JITC and NPS during the summer of 1999. Several dozen government personnel and contractors at JITC were contacted for the study. A common theme that emerged from these contacts is that there remains much work to be done on the foundations of joint interoperability testing, especially as new paradigms in information technology continue to emerge. Virtually everyone who was contacted indicated that they would welcome collaborative engagements with NPS aimed at improving the joint interoperability testing process.

Possible areas of collaboration between NPS and JITC include statistical aspects of the design and analysis of interoperability tests; modeling and simulation (M&S); software testing and reliability; data correlation, fusion, and deconfliction; information operations, assurance, and warfare; electronic key management systems, encryption, and network security; human factors engineering; intelligence interoperability; analysis of joint exercises; and, missile systems interoperability. In particular, the M&S community at NPS will find significant opportunities to develop tools that can be used for the interoperability testing of complex, networked C4I and AIS systems. JITC has also expressed a desire to have NPS develop educational products for its personnel.

Table of Contents

Introduction and Overview	ii
The Mission of JITC	ii
Areas of Mutual Interest	iv
Meeting Different Institutional Needs	v
Security Issues	vi
Points of Contact and Support	vi
1. Interoperability Testing: Concepts, Design and Data Analysis	1
1.1 Experimental and Test Design	2
1.2 Multivariate Data Analysis	4
1.3 Measuring Performance	4
2. Modeling & Simulation: Its Role in Interoperability Testing	5
2.1 Specific Systems and General Issues	6
2.2 The High Level Architecture (HLA) and the Defense Information Infrastructure Common Operating Environment (DII COE)	7
2.3 Interoperability of M&S	7
3. Defense Information Infrastructure (DII): Platforms, Products, and Systems	8
3.1 DII COE	8
3.2 Global Command and Control System (GCCS)	9
3.3 GCCS Common Operational Picture (COP)	11
3.4 Global Command and Support System (GCSS)	12
3.5 Defense Messaging System (DMS)	12
4. Information Operations	13
4.1 IA Testing	14
4.2 IW Testing	14
4.3 IO Testing	14
4.4 Security and Encryption	15
4.5 Y2K Testing	15
5. Other Possible Research Areas	16
5.1 Software Interoperability	16
5.2 Intelligence Interoperability	17
5.3 Missile Interoperability	18
5.4 Joint Exercise Support	19
6. NPS Educational Outreach	20
List of Acronyms	21

Introduction and Overview

The Joint Interoperability Test Command (JITC), located at Fort Huachuca, AZ, is responsible for testing and certifying that command, control, communications and computers intelligence (C4I) systems and automated information systems (AIS) are interoperable between the Department of Defense (DoD) service branches. Determining whether a C4I system is interoperable raises functionality issues that go beyond operability alone. A communications or computer system standing alone may be fully operational, yet fail to "handshake" properly with another operational system. Interoperability failure can have serious consequences for warfighters, who increasingly depend on C4I tools for rapid decisionmaking.

The purpose of this paper is to identify possible areas of collaboration between JITC and the Naval Postgraduate School (NPS). In the summer of 1999 the author visited JITC for a period of two weeks. During that time, he had the opportunity to meet with JITC government personnel and contractors representing many of its areas of activity. There was general agreement that involvement by NPS faculty and students in problems related to interoperability testing would enhance the fulfillment of JITC's mission. The potential therefore exists to develop a working relationship that would be beneficial to both institutions.

The Mission of JITC

JITC is a line organization within the Defense Information Systems Agency (DISA). The JITC mission is "to support the warfighters in their efforts to manage information on and off the battlefield." This includes:

- Being an independent operational test and evaluation/assessor of DISA, and other DoD C4I and acquisitions
- Identifying and solving C4I and Combat Support Systems interoperability deficiencies
- Providing C4I joint and combined interoperability testing, evaluation and certification
- Bringing C4I interoperability support, operational field assessments, and technical assistance to the commanders in charge (CINCs), services, and agencies
- Providing training on C4I systems, as appropriate.

JITC is responsible for certifying that all DoD C4I systems are interoperable, as stipulated in DoD Directive (DoDD) 4630.5, DoD Instruction (DoDI) 4630.8, and Joint Chiefs of Staff Instruction (CJCSI) 6212.01A. DoDD 4630.5 and DoDI 4630.8 mandate joint and combined interoperability certification testing for "all Command, Control,

Communications, and Intelligence (C3I) systems developed for use by US forces." CJCSI 6212.01A expanded the scope to C4I systems and outlined the process that JITC follows with respect to accomplishing its joint interoperability test and certification mission.

To fulfill its mission, JITC has developed extensive test facilities at Fort Huachuca headquarters. For this reason JITC has been classified as an element of the Major Range and Test Facility Base (MRTFB) by DoD. In addition to its Fort Huachuca facilities, JITC conducts much of its testing off-site in distributed networks. JITC operates and controls the Defense Information Testbed (DIT), an extensive network of military, commercial, and Allied test facilities interconnected by high data rate carrier circuits as well as radio and satellite links. JITC also has test facilities in Indian Head, MD and Arlington, VA.

Interoperability testing and certification is a process that originates with the identification of system requirements during the acquisition phase and continues until the system is retired. Products and systems that come under the scope of JITC's certification mission are highly diverse. They include, but are not limited to, radio communication devices, satellite communication systems, commercial off-the-shelf (COTS) software products, software products developed specifically for DoD, financial management systems, missile defense systems, and large-scale networked C4I and AIS systems such as the Defense Messaging System (DMS) and the Global Command and Control System (GCCS). As the only DISA-approved Year 2000 (Y2K) test facility, JITC also conducts extensive Y2K testing of C4I systems and software.

Customers that submit products for interoperability certification include DoD, other federal agencies, and private entities. The facilities and services of JITC are made available to its customers on a cost-reimbursable basis. In order to avoid redundancy in testing, JITC may utilize operational test data from other facilities, including the test and evaluation offices of DoD service branches. In some instances results from developmental testing are "credited" to interoperability testing.

The interoperability testing process begins with the review of a Mission Needs Statement (MNS) and/or Operational Requirements Document (ORD) to identify interoperability criteria. In standards conformance testing, the Joint Technical Architecture (JTA) is consulted to identify the standards that are applicable to the product under test. These criteria or standards are used to formulate a Test and Evaluation Master Plan (TEMP), which when executed yields data on the performance of the product. Test data are used to determine the certification level of the product. Because of the diversity of products that fall under the scope of JITC's mission, there is not a single "standard" approach to interoperability testing and certification. Test designs and the data they produce vary markedly with the product or system.

As suggested earlier, interoperability is a dynamic quality. When the operating system on a computer network is upgraded, a software product that was certified as interoperable on the old system may not be interoperable on the new system. Or, if the

software itself has been upgraded, similar issues arise. For this reason, certification is granted for a fixed period of time, or until changes occur to the product or system that could affect interoperability, whichever is shorter. Products must be submitted for re-certification throughout their life cycles.

Joint Vision 2010 recognizes interoperability as an increasingly important capability of future DoD systems. Future military operations will increasingly utilize network-centric "systems of systems" architectures that require greater interoperability, not only between DoD service branches, but also between U.S. and allied forces. The interoperability goals set forth in Joint Vision 2010 suggests that interoperability testing will remain a key DoD activity well into the foreseeable future.

Areas of Mutual Interest

Interoperability testing touches on subject matter that spans a range of research interests that are represented at NPS:

- Reliability testing involves experimental design and the statistical analysis of test data.
- Software interoperability testing requires knowledge of software engineering principles.
- Testing a large communications or missile system for interoperability suggests the use of modeling and simulation when live testing on a practical scale is not feasible.
- Testing a computerized battlefield visualization system for interoperability raises complex issues in data fusion, and manual integration of information streams with varying security requirements.
- Testing the security of a computer network, including encryption and electronic key management systems, requires knowledge of information assurance issues at the most current state of technology.

These and other subjects related to interoperability testing are discussed further in the remainder of the paper. The point to be made here is that interoperability testing and related activities at JITC pose problems that are "cutting edge" in the fullest sense. NPS faculty and thesis students from a range of disciplines should find many of these problems to be professionally challenging.

The purpose of this paper is to create awareness in a range of subject areas, rather than to give specific research or thesis topics. The author of this paper, trained as a statistician, is not an expert in computer science or information technology, which are two areas that hold significant promise for NPS-JITC interaction. An attempt was made to describe problem areas at a level that gives experts a basis for seeking further

clarification. It is suggested that interested parties contact JITC to learn more about research opportunities in specific subject areas.

Meeting Different Institutional Needs

It is clear that NPS and JITC would bring different objectives into a working relationship. For NPS, the promotion of faculty research and the Masters degree program are its primary objectives. Conducting high-quality research on problems of interest to DoD fulfills the professional aspirations of faculty. Faculty research, in turn, is the conduit through which NPS students gain exposure to challenging problems at a level appropriate to their training. Both faculty and student research add value to the operations of DoD, and constitute an in-house base of expert knowledge that is adaptable to changing circumstances.

For JITC the primary objective is to fulfill its interoperability testing mission. JITC personnel are well-trained professionals who take a keen interest in subjects related to their work. But from JITC's perspective, the objective of research is to contribute materially to its mission within a reasonably short time frame. For NPS, dealing with DoD sponsors that take a utilitarian view of research is nothing new, but it is worth emphasizing this point for faculty members who wish to work on projects sponsored by JITC.

Additionally, JITC sees a working relationship with NPS as a means of gaining exposure among active duty military officers, some of whom would hopefully return to JITC upon graduation. Establishing a pipeline of talented, well-educated military officers from NPS to JITC would be beneficial to both institutions. NPS graduates bring visibility to technical problems at DoD organizations where they serve, which promotes additional NPS research and student interest, which in turn makes these organizations attractive to NPS graduates who want to have their newly acquired skills put to good use.

However, it is not possible to develop this pipeline without the active participation of NPS faculty. NPS students must complete the requirements of the Masters degree in less than two years. In order for students to produce DoD-relevant, thesis-quality work on schedule, it is necessary for faculty to be involved with the subject matter. In addition to bringing problems to the attention of students in search of thesis topics, faculty participation ensures that students are not cast adrift, or burdened with problems that are beyond their capabilities. It also provides continuity in attacking problems that require sustained effort over a period of time.

For these reasons, a working relationship between NPS faculty and JITC must lay the foundation for a broader-based relationship that includes NPS students. How faculty involvement is structured depends on the cooperation of individual faculty members with JITC and/or with other organizations that sponsor research in interoperability testing.

Security Issues

Activity at JITC ranges from unclassified to the highest classification levels, depending on the system or product being tested. NPS faculty and students who wish to become involved in JITC-related work need to be aware of the level of security clearance required for a particular project.

Points of Contact and Support

Faculty who wish to learn more about research opportunities at JITC should contact the JITC Deputy Commander, Mr. Denis Beaugureau, at (520) 538-5000 (DSN 879-5000), e-mail at beaugurd@fhu.disa.mil, or the JITC OT&E Test Director, Randon Herrin, at (520) 538-5091 (DSN 879-5091), e-mail at herrinr@fhu.disa.mil. It is recommended that an interested party begin by reviewing the JITC homepage at <http://jitc.fhu.disa.mil> to obtain current information about the scope of activities at JITC. Under the JITC homepage the web site at <http://jitc.fhu.disa.mil/sitemap.htm> is an especially useful resource for this purpose.

Other organizations within DISA may be willing to sponsor projects related to interoperability testing. The DISA Organizational Staff Home Page at <http://www.disa.mil/org/disastaf.html> describes the organizational structure of DISA and gives points of contact.

Modeling and simulation (M&S) plays a significant role in interoperability testing. The D8 (C4I Modeling, Simulation, and Assessment) staff at DISA may be contacted about projects involving M&S in interoperability testing and related issues. DoD has many organizations promoting the use of M&S from a variety of perspectives. These include the Defense Modeling and Simulation Office (DMSO) and branch-specific M&S offices. Links to many of these offices can be made from the DMSO web site at <http://www.dmso.mil>. The M&S community at NPS also may be able to provide useful, up-to-date information on support for projects in this area.

The Institute for Joint Warfare Analysis (IJWA) at NPS has an interest in interoperability issues, and resources for faculty support. Professors William Kemple or Gordon Schacher should be contacted for additional information.

The Director, Operational Test & Evaluation (DOT&E) may also be able to provide information on support for work related interoperability testing. The DOT&E homepage is <http://www.dote.osd.mil>.

1. Interoperability Testing: Concepts, Design and Data Analysis

As part of the larger operational test and evaluation (OT&E) paradigm, the interoperability testing process is similarly structured. Each step of the process has to meet rigorous specifications:

1. ***Interoperability is defined for the product or system at hand.*** Interoperability is often not clearly defined in a Mission Needs Statement (MNS) or Operational Requirements Document (ORD). The concept itself may be difficult to define objectively or within a fixed scope. For instance, what does interoperability mean for a C4I or AIS system when the number of permutations of its nodes is exponentially large?
2. ***Measures of performance (MOP) are defined.*** When interoperability entails conformance to quantitative or binary (yes/no) military standards the MOPs may be defined accordingly. But for many C4I or AIS systems such standards do not exist. Quantitative measures may be used, such as the time required to transmit an e-mail message over a computer network, to capture some of the meaning of interoperability. Other aspects of interoperability are not easy to quantify. For example, does the symbology used in a combat visualization system confuse human end-users?
3. ***Test scenarios are designed that are as true as possible to the interoperability requirements of the product or system.*** Designing realistic operational tests of a C4I or AIS system can pose difficult problems. Time, money, and logistical constraints often prohibit the live testing of such systems. In the laboratory, achieving the same scale and complexity of a live-use system may not be possible. Given these factors, what is the best way to design test scenarios that are reliable indicators of how well the system is likely to perform in practice?
4. ***Testing is conducted so that the test data are sufficient in quantity and quality to allow conclusions to be drawn.*** Testing the same system repeatedly does not normally produce the same results each time. How many repetitions of a test are needed to give statistically reliable estimates? And, how should the test scenario be varied in order to obtain a reliable description of performance both between and within test scenarios?
5. ***The test data are used to determine the certification level of the product or system.*** How can the test data be summarized to communicate the interoperability status of a C4I or AIS system?

Possible research areas:

Each step in the testing process is subject to refinement as the concept of interoperability evolves with the products and systems it addresses. JITC also believes that its basic approaches to test design and data analysis may be improved through concerted research. NPS can help to improve the conception, design, and analysis of interoperability tests in several areas:

1.1 Experimental and Test Design

JITC does not use "classically" designed experiments in its test procedures. The number of tests that are done and manner in which they are designed are dictated by limitations of time, manpower, and money. It would be easy to contemplate test designs that increase the expenditure of these resources, and in some instances such increases may be necessary to achieve the objectives of testing. However, it is also useful to ask if better tests can be designed with the same level of resources.

Testing the Defense Messaging System (DMS) provides an illustration. DMS is an integrated collection of COTS software products, designed to run on the Defense Information System Network (DISN), for the purpose of serving as the single DoD-wide system for electronic messaging, replacing AUTODIN and legacy e-mail systems. DMS is also discussed in section 3.5 below. With millions of potential end-users of the system, it is not possible to test DMS for interoperability under every possible traffic configuration. Given that this is the case, how should DMS be "stimulated" in interoperability testing so that success/failure in testing is reasonably indicative of success/failure in practice?

As a system that is not yet fully employed, DMS cannot be live-tested in its final operational state. But many aspects of DMS interoperability can be captured in laboratory testing with the use of automatic loading tools. JITC has initiated such testing by stimulating a facsimile of DMS with different types of messages under traffic loads of varying intensity. Orderly, nonstochastic stimulation of this type may reveal faults with the system or software at its early stages, but the issue of interoperability under the stress of actual traffic loads is only partially addressed.

Designing a realistic operational test of DMS, using laboratory or distributed resources, that is at the same time compatible with the mission of JITC would be a significant challenge. Such a test using Modeling & Simulation (M&S) tools would need to satisfy Verification, Validation, and Accreditation (VVA) requirements. Validation means that the method of stimulating the system under test must be justified as having an operationally valid basis. Accomplishing this would require an understanding of traffic load patterns on DoD messaging systems, perhaps obtained from analyses of historical traffic load on similar systems, provided that such data are available.

At a more basic level, experimental design addresses problems of sample size selection and the varying of factors that affect outcomes. Much of the testing at JITC uses MOPs consisting of the number of times a task was successfully executed. For example, if a message was transmitted 100 times and successfully received 93 times, the MOP would be $p = 93\%$, which is also an estimate of the "true" successful transmission rate π under a Bernoulli model. If the Bernoulli events are statistically independent, p is a binomial random variable divided by the number of trials. This fact can be used, for instance, to determine the number of trials needed so that p and π differ by less than two percentage points with 95% probability. Similarly, if π_0 is a threshold value that implies acceptability, the minimum sample size can be found such that, if $\pi_0 - p$ is less than two percentage points, then π is less than π_0 with 95% confidence.

In practice, however, determining the sample size and resulting probability or confidence level may be complicated by positive correlation of the trials. JITC mentioned that failures are often clustered, with tests conducted in succession tending to have low variability in their outcomes. This would imply that standard calculations understate the sample sizes needed to make statements of the type described above.

Conversely, JITC has found that variability is greatest between different testing configurations. When multiple factors or control variables affect the MOP, it is therefore desirable to test a large number of factor configurations with few replications per configuration rather than vice versa. If the number of factors is large, performing a "full-factorial" experiment of all factor levels intercrossed is not practicable. In testing the Global Command and Control System (GCCS), for instance, approximately 12 factors are considered. Even if there were only two levels per factor, the total number of possible configurations would exceed 4,000. A more realistic objective is to test a subset of configurations, subject to resource constraints, that gives the most informative picture of interoperability.

Several JITC personnel expressed the belief that JITC collects too much test data in some areas, and not enough in others. This may be a reflection both of correlation and the manner in which tests are designed. There are several areas in which NPS research may lead to more efficient employment of testing resources. One would be to undertake a study using historical test data at JITC to develop test designs that take correlation into account. Another would be to use design of experiments principles to develop efficient test designs in multifactor testing.

1.2 Multivariate Data Analysis

Test data are analyzed by JITC using an essentially univariate approach. Contractor personnel calculate summary statistics and create graphical displays without taking into account interdependence of the MOPs. But a series of univariate analyses can miss valuable information that a multivariate approach can bring to light. For example, suppose that a test uses 50 MOPs that are highly intercorrelated, to the extent that a subset of 15 of them contains the same information. By identifying this subset and eliminating the other 35 MOPs from test the plan, time and money can be saved without compromising the quality of the test.

JITC has received comments that a multivariate approach should be considered, but the idea has not been pursued, in part because of time and staff limitations. Since testing is not designed to generate data for multivariate analysis, attempting to conduct such analyses after the fact may encounter unforeseen problems. Nonetheless, it would be worthwhile for NPS to explore this concept, initially at the faculty level only, to determine if existing data are suitable for progress to be made in this area.

1.3 Measuring Performance

MOPs are designed to capture the meaning of interoperability in the usage context of the product or system. Some aspects of interoperability may entail conformance to a set of standards spelled out in the JTA. Usually, however, it is up to JITC to define MOPs based on its understanding of the operational requirements for the product or system. If a high rate of success is required for a particular aspect of performance, JITC may require that a 95%, 99%, or even 100% success rate be observed in a laboratory test. One of the concerns that JITC has raised is that it often sets these percentages without a systems perspective. Ideally, what is tolerable as a failure rate should depend on the impact of failure on the warfighter, and on the accumulation of risks that may lead to a system failure. A project that may be of interest would be to study a system that JITC has tested and analyze its MOPs from the point of view of warfighter needs and overall system performance.

MOPs can be hard to define objectively, which is why JITC sometimes relies on the appraisals of subject-matter experts (SMEs) to define its test criteria. This is particularly the case when ease or efficiency of use of a C4I system by a human agent is the criterion of interest. Asking an expert to try out the system and report his or her opinions may offer useful insights, and it may even be the only reasonable way to measure some aspects of performance. To the maximum extent possible, however, it would be desirable to construct objective measures of performance. One approach in this direction would be to use human factors principles to define measures of usability by humans of a C4I system. NPS has a research presence in the area of human factors, particularly in its relation to human vision.

2. Modeling & Simulation: Its Role in Interoperability Testing

M&S plays an increasingly important role in many areas of DoD activity. It represents a technology-rich approach to solving problems that would otherwise be intractable, and it often has the potential to do so at substantially lower cost than its alternatives. Developing M&S as an interoperability testing tool has the potential to provide the basis for many NPS-JITC collaborative projects.

Although M&S is well-suited to testing many of the C4I and AIS systems that fall under the scope of JITC's mission, justifying its use for a particular test is not a simple process. Meeting the Validation, Verification, and Accreditation (VVA) standards that apply to any DoD M&S application has unique implications when it is used in interoperability testing and certification.

JITC has an extensive infrastructure to support the use of M&S in interoperability testing. A full description can be found on the JITC web site at <http://jitic.fhu.disa.mil>. JITC's hardware-in-the-loop distributed test network includes the following components that support its M&S activity:

- Joint Interoperability Evaluation System (JIES) and the Joint Tactical Data Link Laboratory (JTDL) Network. These components support distributed simulations, and give JIES the potential to join a federation of models and live systems that can support the test of such systems as Theater Ballistic Missile Defense or National Missile Defense.
- Global Command and Control System (GCCS). GCCS is discussed more extensively in section 3. The JIES/GCCS interface allows JIES-simulated scenarios to be displayed on GCCS.
- JIES External Model Interface. This interface gives JIES the capacity to translate Tactical Digital Information Link (TADIL) messages for use in outside simulations, and to translate data from outside simulations into simulated sensor input to live tactical data systems in the JTDL Network.
- Simulated Warfare Environment Generator (SWEG). The JIES/SWEG interface, which provides realistic scenarios and stimuli to tested systems, is used in TADIL certification testing at JITC.
- Joint Theater Level Simulation (JTLS). JTLS can be used to drive GCCS to provide realistic combat scenarios. The GCCS/JTLS interface converts JTLS output to Over-the-Horizon (OTH) Gold messages, which GCCS accepts and displays on the GCCS Common Operational Picture (COP).

In addition to these tools, JITC also uses a variety of communication system stimulators including those for testing tactical switches, FTP and SMTP transfers, the Tri-Tac family of message switches, and the Defense Messaging System (DMS). Its assessment tools include PreVue-X, COMNET, NETSYS, Best/1, and OPNET.

JITC has been designated the Responsible Test Organization (RTO) for the System Capable of Planned Expansion (SCOPE) Command. In this role, JITC provides M&S and testing support to the High Frequency Global Communications System Program Office. JITC's near-range plans call for an expansion of its M&S facilities to support interoperability testing.

Possible research areas:

There is a firm base of support for M&S at NPS, as indicated by the levels of both faculty and student research in this area. The recently developed Modeling, Visual Environments and Simulation (MOVES) curriculum at NPS is evidence of this commitment. For NPS, an extension of its M&S activity into the area of interoperability testing would offer new paradigms and challenges. For JITC, the expertise that NPS can offer would be a valuable addition to its testing programs.

2.1 Specific Systems and General Issues

Specific systems for which M&S is either being used in, or may enhance interoperability testing are discussed in subsequent sections of this paper. These include GCCS, GCSS, DMS, and the Theater Missile Defense (TMD) Family of Systems (FoS). Each of these systems presents opportunities for NPS and JITC to collaborate on the development of M&S tools for interoperability testing and certification.

M&S tools designed for use in interoperability testing must generate realistic operational scenarios, as described in a MNS or ORD for the system under test. Developing such tools has been and will continue to be fertile ground for research. Generally, JITC approaches the use of M&S in its testing programs cautiously, due to developmental costs and the conceptual difficulties that it sometimes poses. M&S proponents at NPS may wish to explore these issues with JITC in more detail.

Nonetheless, there is general agreement at JITC that M&S has a significant role to play in testing the multifaceted array of C4I and AIS systems that come under JITC's mission. For some systems, such as DMS or TMD FoS, testing under live or full-scale conditions is impractical. For others, there is a need to extrapolate small-scale laboratory test results to larger, operational scales. M&S has been used to expose system faults and to trace them to specific causes. JITC was able to locate the source of problems in the Defense Travel System that led to unacceptable delays when it was tested using M&S.

2.2 The High Level Architecture (HLA) and the Defense Information Infrastructure Common Operating Environment (DII COE)

The HLA is a mechanism, sponsored and under development by DMSO, for ensuring the interoperability of distributed simulations. DII COE, defined in section 3, is a collection of software products that meet certain standards so that C4I systems are portable and interoperable across compliant platforms. There is interest, expressed both by DISA (D8) and DMSO, in finding a strategy so that the HLA can be merged with DII COE. As one DISA official stated: "This is something I need now and has the highest level of interest." There has already been work in this area by the Army Modeling and Simulation Office (contact: LTC Don Timian), but the same DISA official suggested that new projects would also be considered.

Including the HLA runtime interface (RTI) as a utility of DII COE would provide a seamless interface between the real and simulated worlds. C4I systems that are DII COE compliant would be "ready made" to interface with M&S tools for training and testing purposes. Real and simulated data would be interchangeable and capable of display using the same tools. And, the interoperability of simulations would be maintained throughout the DII COE architecture.

JITC identified several issues that must be addressed to successfully merge the HLA and DII COE:

- Determine which C4I systems can interoperate via a standard HLA RTI
- Develop a standard Federated Object Model (FOM), RTI interface, or extensions that would facilitate interoperability
- Identify additions or modifications to DII COE standards that are necessary to bring about the merger.

2.3 Interoperability of M&S

As stated in the previous subsection, the purpose of the HLA is to enhance the interoperability of M&S applications. The DoD Modeling & Simulation Master Plan (DoD 5000.59-P) places heavy emphasis on the concept of interoperability. Although M&S interoperability is not currently considered to be part of JITC's mission, M&S and C4I interoperability are sometimes intertwined. An example is given by Simulation Based Acquisition (SBA), with its sharing of testing and training assets and loss of distinction between testing phases.

JITC has had some, but limited, success in building a M&S interoperability testing program. Given JITC's resources in the M&S area and its experience in interoperability testing, NPS faculty or students who are interested in M&S interoperability issues may find it productive to contact JITC.

3. Defense Information Infrastructure (DII): Platforms, Products, and Systems

The Defense Information Infrastructure (DII) is a "system of systems" that aggregates all DoD communication networks, sensors, data entry devices, computer resources, facilities, and operational and support staff for the collection, production, storage, display, and dissemination of information to DoD end users. Interoperability is clearly at the core of DII, and JITC is extensively involved in the life-cycle testing of DII systems. For this purpose JITC has developed the DII Test Network, a distributed platform consisting of the JITC facilities at Fort Huachuca, service and agency facilities, and commercial and allied testbeds located throughout the world.

The DII Common Operating Environment (COE) is a collection of software products categorized into three layers: the kernel, infrastructure services (data exchange), and common support applications. The purpose of DII COE is to provide an environment in which DII mission applications are portable between platforms. Compatibility of an application with DII COE is determined by testing to standards set forth in the Integration & Run Time Specification (I&RTS). There are eight compliance levels (1 = low, 8 = high), with levels 5 and higher currently qualifying for DII COE compliance. Additional information on DII COE and I&RTS can be found on the DISA web site at <http://www.disa.mil>. JITC will begin testing for DII COE compliance in the near future.

DII supports a number of large-scale, software-intensive systems, including the Global Command and Control System (GCCS), the Global Combat Support System (GCSS), and the Defense Messaging System (DMS). JITC is extensively involved in either testing or planning to test these systems in the near future.

Possible research areas:

The scope and complexity of DII systems offer many opportunities for collaboration between NPS and JITC. With strong student and faculty interest in the Information Technology (IT) area, and excellent computing resources that includes access to GCCS, NPS would bring significant capabilities to any collaborative effort.

3.1 DII COE

Currently, there are several laboratories in the U.S. that perform testing for DII COE compliance. While some of the standards set forth in the I&RTS are objectively testable, others are less so. This subjectivity means that a product certified at a particular level by one laboratory may fail certification by another. Also, the relationship between DII COE compliance and interoperability is not yet fully understood. JITC and its contractors have identified several problem areas that if

successfully addressed could help JITC to integrate a DII COE testing program with its interoperability testing mission more effectively.

One possible project would be to examine the I&RTS to identify which standards are, and which are not, necessary for interoperability of a DII application. DII COE compliance is neither a necessary nor a sufficient condition for interoperability, although individual standards may play an important role. Knowledge of a major DII application such as GCCS may serve as the basis for making a detailed assessment of the I&RTS as it affects that system.

Both JITC and the DII COE testing community are interested in the development of automated testing tools. JITC noted that DII COE compliance testing is time-consuming and burdensome because of the lack of such automation. Effort has already been made in this area, notably by SPAWAR on a task from DISA (contact: Jack Chandler). It was reported that this automated testing software, written in JAVA and PERL, has successfully tested up to 80 percent of the specifications needed for level 5 compliance. JITC may welcome an independent assessment of this tool, or even the development of a new automation tool if it is better suited to the kinds of testing that JITC plans to conduct.

A JITC contractor made the observation that database applications in DII COE are more problematical than other types of applications. Interested parties may want to follow up on this comment to learn more about the nature of the problem.

3.2 Global Command and Control System (GCCS)

GCCS is an automated information system, designed to operate in the DII COE environment to support deliberate and crisis planning with the use of an integrated set of analytic tools and data transfer capabilities. The development objective is for GCCS to become the single C4I system to support the warfighter from foxhole to command post.

JITC conducts extensive interoperability testing of GCCS and the applications associated with it. The MOPs it uses to assess interoperability are both objectively and subjectively based, the latter consisting of subject-matter expert (SME) appraisals. JITC has mentioned a number of potential problem areas in which it would welcome input from NPS:

- Software virus protection between interfaces is a significant interoperability concern with GCCS. What is the nature and scope of this threat both in general and on specific interfacing systems, including the SIPRNET? Should JITC be testing virus protection software, and if so, how should such testing be conducted?
- What are the interoperability issues for software virus protection when different platforms (e.g. Solaris, HP, PC, Macintosh) are interconnected?

- What are the interoperability issues for software virus protection as they concern FTPs and other manual data exchanges? Or, automatic exchanges involving databases?
- Much of JITC's testing of GCCS concerns timeliness measures, such as the length of time needed to login to a system. Are these measures suitably defined and assessed in relation to what is needed for mission accomplishment?
- Specifically, which elements should be timed? GCCS raises man-in-the-loop issues as well as purely electronic ones. If the former are to be included, can relevant MOPs be defined?
- Scalability: can tests designed for normal usage conditions be extrapolated to an n -fold increase in usage? An example would be access to GCCS through the SIPRNET.
- Incrementally developed and fielded C4I systems such as GCCS have no clear interoperability requirements. How can data on reliability, availability, and maintainability (RAM) be obtained for such systems?
- It would be of interest to compare GCCS to its predecessor. Does it perform at least as well? As GCCS have developed and improved with technology, requirements from users have also increased ("requirement creep"). Has GCCS adapted well to the greater demands placed upon it?

NPS has a 512 kilobit SIPRNET link to GCCS, although it may lag somewhat in the upgrade stream. This may be sufficient for NPS students or faculty to conduct much of its collaborative work using its own facilities.

Several other potential areas for research are also worth mentioning. Reliance on SME appraisals, while understandable and certainly appropriate for a system like GCCS, nonetheless lends an air of subjectivity to testing. If it were possible to design objective measures that captured the same information, the consistency of test data would be improved. It would be interesting to review the SME-based MOPs for a system like GCCS to determine the extent to which objectification is possible.

A better grounding in Human Factors principles may lead to better interoperability assessments in some areas. There is concern that increasing the complexity of some systems may degrade interoperability if human actors cannot cope with the sensory demands placed upon them. On the other hand, test subject claims that "this is too much" or "this does not overwhelm me" may not bear up under practical usage. Having NPS faculty and students study these issues as problems in Human Factors may lead to the design of more objective MOPs.

As a large, heterogeneous C4I system, the interoperability issues that are central to GCCS are difficult to replicate in a laboratory. Modeling & Simulation (M&S) is

therefore a viable option for GCCS testing. JITC has developed an infrastructure for M&S support that includes the Joint Interoperability Evaluation System (JIES) and Joint Tactical Data Link Laboratory (JTDL). In particular, JITC developed a JIES/GCCS interface that allows display of a JIES test scenario on the GCCS Common Operational Picture (COP), and a JIES interface with the Simulated Warfare Environment Generator (SWEG) which can then be used to drive GCCS. GCCS is one of a number of systems that offers NPS the opportunity to collaborate with JITC on developing a linkage between M&S and interoperability testing. M&S is discussed further in section 2.

3.3 GCCS Common Operational Picture (COP)

COP is a GCCS application that provides commanders and operators a "common graphical description" of the battle space in an area of operations. It includes (1) current locations, planned movement information, and amplifying information on friendly, neutral, and enemy units (air, sea and ground); and (2) generated features and projections (e.g., battle plans, operating zones, fly-through depictions). COP makes extensive use of sophisticated computer graphics, and through GCCS it integrates information from a variety of sources from the Secret to the Top Secret/SCI (TS/SCI) security levels. Significant enhancements to COP are planned over the next several years.

As a GCCS application, the comments made in the previous subsection also apply to COP. In addition to these JITC mentioned several issues in the context of COP that would benefit from additional investigation:

- Data correlation/fusion/deconfliction. When data are received from multiple sources, they may conflict in certain respects or not be synchronized with respect to space or time. Resolving such disparities is important if a "common operational picture" consistent with the state of information at a given point in space and time is to be formed. This is a challenging problem area that combines electrical engineering, physics, and mathematics with computer science and information technology.
- Man-in-the-loop testing. Input to COP consists of Secret and TS/SCI feeds, but dissemination may require a step-down below the TS/SCI level. Merging of the two types of input requires human intervention, which effectively creates an "air gap" between the Secret and TS/SCI levels of COP. Generally, ensuring the fidelity and timeliness of command and control (C2) operations through COP are challenging problems. The interoperability testing of such systems raises issues that have not been fully resolved.
- Modeling & Simulation. JITC has initiated testing of the COP using M&S tools. Given the large number of potential situations in which COP may be used, the development of a set of M&S tools for COP interoperability testing should offer many opportunities for collaboration between JITC and NPS.

- The concept of interoperability for COP. What precisely does it mean to say that COP is interoperable? Different users of the system may have different answers, depending on their needs. A potential project would be for NPS to review the current concept of interoperability used in COP testing from the perspectives of warfighters and other system users, and/or to develop alternative concepts.
- The concept of COP for interoperability. To what extent can COP be used to test the interoperability of C4I products and systems?

3.4 Global Command and Support System (GCSS)

GCSS is a DII COE command and control (C2) system being developed to serve as the analog of GCCS in the areas of logistics, medical finance, personnel and other functional areas. It is on a developmental track similar to GCCS, but lagged approximately four years. JITC plans to use the same testing strategy for GCSS as it does for GCCS. Together, GCCS and GCSS are the two most important testing programs on JITC's horizon. For NPS, GCSS may offer a wide variety of opportunities to collaborate with JITC at the ground level of interoperability testing. The same issues discussed in sections 3.2 and 3.3 may apply to GCSS in the near future.

3.5 Defense Messaging System (DMS)

DMS was defined and discussed in section 1.1. A problem of general interest is to develop methods for stimulating DMS in testing so that the system is stressed under conditions that are as close to actual usage as possible. Since testing a "live" DMS is not possible, M&S is a promising testing approach for this system. Other problem areas include scalability of test results to actual usage loads, and software reliability including vulnerability to software viruses.

4. Information Operations

Information Operations (IO) is a concept that encompasses Information Assurance (IA), Information Warfare (IW), encryption, security management, Y2K testing, and other activities concerned with preserving the integrity of DoD information, and the denial of information capabilities to adversaries. But IO is not considered to be merely the union of its constituents. The often-expressed view is that IO is about information, as distinguished from the systems that serve the needs of information. JITC has a dedicated group that is attempting to define interoperability as it applies to this new and evolving field.

Some of the interoperability testing in this area deals with standards compliance, as in the testing of software developed by contractors and vendors for compliance to the DoD PKI standards. Similarly, Y2K testing addresses well-defined objectives. As its own entity, however, IO is a fluid concept for interoperability testing, particularly when attempting to translate its information-centric philosophy into testing principles. Opinion at JITC varies on the extent to which this philosophy can be made practicable.

IA interoperability recognizes that C4I or AIS systems may be subject to infiltration or corruption by adversaries, or have their security breached inadvertently. When successful strategies for dealing with these problems are found, adversaries devise new methods of attack. This suggests that IA interoperability is inherently dynamic. The virus protection software that was effective last month may be worthless today, and given enough time some hackers manage to get past whatever new firewalls are built.

JITC is actively involved in testing IA tools, including the IA Common Operational Picture (IA COP), which is a collection of about 30 security tools for protection, detection, reaction, and restoration when a DII system is confronted with an information threat. Testing emphasizes functionality, security, performance, interoperability, Y2K, usability, bandwidth, improvements, and enhancements.

As mentioned in the introduction to this paper, JITC is the only DISA-approved Y2K test facility. In this capacity JITC conducts extensive Y2K testing of C4I systems and software. JITC is also an independent DoD testing agent for the National Security Agency (NSA), for which JITC conducts, witnesses, and reports on testing efforts conducted on the Electronic Key Management System (EKMS). Future JITC testing will concentrate on end-to-end EKMS interoperability to help ensure its full operational capability in the third quarter of FY 2000.

Possible research areas:

There are potential opportunities for NPS to work with JITC in developing the concept of IO/IA/IW interoperability testing. From discussions with JITC government personnel and contractors, it appears that IO and some of its constituent fields have evolved too rapidly for the testing and evaluation (T&E) communities to keep up. At the

same time, JITC has found it difficult to hire and retain qualified IT personnel in this highly competitive job market. These factors give NPS the opportunity to conduct research on problems of concern to JITC that might otherwise receive little attention.

4.1 IA Testing

Although JITC is actively involved in IA testing, the general feeling is that a comprehensive IA T&E process has not yet been defined. The IA testing process needs better defined test requirements (including interoperability) and metrics, test plans, tools, and methods for analyzing test results.

JITC has expressed that it wants to conduct some of its IA testing using a multi-tier laboratory architecture with "hacker enclave." It may be interesting for NPS to consider what types of architectures involving hostile actors can bring realism to IA testing. Can M&S be used to generate valid threat scenarios for use in IA testing?

Validating nontrivial IA threat scenarios is conceptually difficult. JITC noted that the greatest threat is from the "trusted insider" who is beyond the scope of intruder-oriented tools. Good personnel management, including user certification and monitoring, is needed to counter the insider threat.

4.2 IW Testing

The concept of IW testing has not yet been developed. NPS may therefore be able to play a significant role in creating a foundation for IW testing programs. Possible directions include the development of a suite of DII COE-compliant tools (an IW COP?) for this purpose, and to explore the use of M&S to create IW scenarios.

4.3 IO Testing

Developing a set of testing principles for IO interoperability is an essentially untouched problem, due in large part to the elusive nature of information as an object. Should information be viewed as a security issue, or as an asset management issue? The latter is suggested by the Joint Doctrine for Information Operations (JCS Publication 3-13, 1998), which recognizes information as the "warfighter commodity of exchange." Seen in this light, the following questions are posed: To what extent can an analogy be pursued between IO and the functioning of a market? Can information be managed as an asset to be inventoried, prioritized, protected from "embezzlement" and appreciated? And, what are the implications of the answers to these questions for IO testing?

4.4 Security and Encryption

JITC tests electronic keys for conformance to the DoD Public Key Infrastructure (PKI) standards. Contractors and other software vendors achieve a level of interoperability of their products through DoD PKI compliance. In the future EKMS may merge with PKI and expand. One issue with this concept is finding a reliable, standard means to identify persons with a type of ID number. This number must not only identify the person but also his or her access privilege level, which may change over time.

Related security issues are posed by the "Voting Over the Internet" facility, which is currently being tested by JITC. Individuals who vote over the Internet on DoD-relevant matters do so with the expectation that their votes are confidential. To what extent is the secrecy of ballots actually preserved?

An increasingly important security issue concerns the development of DoD web pages. As anyone who has browsed these web pages knows, DoD has an extensive information presence that is accessible to virtually anyone with an Internet connection. DoD web pages are developed autonomously by its organizations and offices, with little systematic control to ensure that the larger strategic interests of DoD are protected in the dissemination of information. One concern that was raised by JITC is that the Internet may in some respects override the chain of command. Is this a significant problem, and if so, what should be done about it?

4.5 Y2K Testing

JITC reported that its Y2K testing efforts have gone smoothly with few Y2K problems detected. The Y2K problem will, hopefully, be moot very soon, but it leaves some interesting questions, such as what will become of the large investment in resources dedicated to Y2K testing? Can they be recycled for other testing purposes? Will there be long-term or ancillary benefits from Y2K testing?

5. Other Possible Research Areas

This section highlights several other areas where JITC is actively involved in testing, and where NPS faculty and students may find opportunities for collaborative research.

5.1 Software Interoperability

Earlier sections of this paper discussed software in the context of particular systems. There are also interoperability testing concerns for software that are generic in nature:

- Fault testing and discovery. Interoperability testing is directed towards requirements derived from an ORD or MNS. JITC does not attempt to "break" a software product above what is necessary to test its requirements. Unanticipated failure modes may, however, affect interoperability. These observations raise some important points: To what extent should interoperability testing of software be devoted for searching for failure modes? And, if a failure is discovered in testing that was not "scripted" but nonetheless is important, how should it enter into the interoperability assessment?
- Testing COTS products. DoD extensively uses commercial off-the-shelf (COTS) software products for building its C4I and AIS systems and networks. An added difficulty in testing a COTS product is that the source code is proprietary. It is therefore not possible to trace a particular problem, such as a segmentation violation, to its origin if that happens to be a particular block of code in one of perhaps many products that are simultaneously tested in a network configuration. Finding better ways or tools to test software products in networks consisting of mixed COTS, GOTS, and DoD software would be an interesting research topic.
- Software patches and upgrades. A C4I network may consist of a large number of operating systems, utilities and applications, each on its own upgrade schedule. When the network is tested for interoperability, certification applies to a fixed configuration of product versions. In practice, individual products are often upgraded on staggered schedules. Periodic re-certification is necessary for these and other systems because they change over time. But, how do incremental changes affect interoperability? A related issue concerns software "patches" that are often distributed without changing the version number, usually to fix a problem that was discovered after commercial release. Research has suggested that patches are often not well validated or "regression tested," and that they have about a 75 percent chance of introducing new flaws. What should the interoperability testing position be with respect to software patches?

5.2 Intelligence Interoperability

Intelligence operations encompass technology, human agents, and procedures for training personnel. Much of JITC's activity in this area is focused on the Department of Defense Intelligence Information System (DoDIIS), which is actually a "system of migration systems" developed individually by the services, and managed by the Defense Intelligence Agency (DIA). The focus of interoperability testing of a DoDIIS migration system, or any intelligence information system, is on the ability to exchange information in sufficient time, by the designated communications means, with the accuracy required by the user to perform assigned missions. The human side of intelligence operations is man-in-the-loop by nature, and therefore difficult to test in a structured framework.

JITC identified several possible topics for NPS research involvement in intelligence operations testing. Funding from DoD for work in intelligence operations is expected to remain good in the near future.

- DoDIIS testing and real performance. DoDIIS testing is a cooperative effort with the Joint Integration Test Facility (JITF) at Rome Laboratories in Rome, NY. Most of the initial "integration" or Beta 1 testing is conducted at JITF, with follow-up testing for additional interfaces conducted at Beta 2 sites. Beta 2 testing often is piggybacked onto other activities, which JITC has found only provides a fraction of the interoperability data that it needs. Perhaps as a result of this, JITC has received complaints from warfighters that the real-life performance of the tested systems is worse than expected. This suggests that there is room for research into better paradigms for testing DoDIIS migration systems.
- Metrics for DoDIIS testing. DoDIIS interoperability testing essentially involves having analysts exchange information over systems, and then asking the users to assess the accuracy, usability, and timeliness of the information received. The test data consist of these survey responses and the messages that were sent and received. Possible topics for research include (1) finding better metrics for interoperability of intelligence information systems, and (2) finding ways to standardize the testing process.
- Development of virtual networks for testing. Another possible area for research is the development of "virtual" or "cloned" networks for testing purposes. Such parallel systems are constructed when it is not possible or practical to disrupt a live system to conduct testing. This concept has been used with success in Y2K testing, but its broader application has not been well embraced. However, DIA currently appears to be favorably disposed towards the idea.

5.3 Missile Interoperability

Theater Missile Defense (TMD) Family of Systems (FoS) is currently in the developmental stage with regard to fielding interoperable systems. TMD FoS spans the Joint Planning Network (JPN), Joint Data Network (JDN), and eventually the Joint Composite Tracking Network (JCTN). The Global Command and Control System (GCCS) will be the backbone of JDN. Interoperability test data are available for JDN and GCCS. However, none of the TMD Major Defense Acquisition Programs (MDAPs, including PATRIOT, THAAD, etc.) or external systems (e.g., GCCS) are currently certified for interoperability with regard to theater missile defense.

JITC has been tasked by the Ballistic Missile Defense Organization (BMDO) to conduct MDAP joint interoperability testing with regard to TMD FoS. This effort is in its early stages, and should continue as a major testing program into the foreseeable future. Since TMD FoS can exist in many different configurations, an all-encompassing interoperability assessment cannot be made. JITC anticipates that its assessments will integrate data from JITC laboratory tests, exercises, M&S, operational tests conducted elsewhere, and Battle Management C4I (BMC4I) tests.

The following are some of the areas in which NPS may be able to collaborate with JITC on the development of TMD FoS testing programs:

- Modeling & Simulation in missile testing. THAAD demonstrated the high cost and policy risks associated with live-testing a major missile system that is still under development. Some have suggested that all of the early failures could have been found with hardware-in-the-loop (HWIL) testing beforehand. The issue is how to generate the right scenarios for HWIL testing to expose failure modes in missile systems. M&S may be useful for solving this problem.
- Integration of exercise and operational test data. Joint exercises such as Roving Sands are not conducted for the purpose of generating interoperability testing data, although they may give useful interoperability information. Nonetheless, joint exercises give some information about how missile systems are configured when the services bring their C4I systems to be interconnected. Thus, exercise data may reveal previously unknown failure modes or interoperability problems under the stress of actual usage. How can exercise data be used to improve or validate laboratory or HWIL testing for missile systems?
- Tactical Digital Information Link (TADIL) certification testing. Most of JITC's interoperability testing effort for missile systems has been in the area of compliance to TADIL standards. Having all systems that comprise TMD FoS be TADIL certified is an important condition for interoperability. Currently, TMD FoS is a mixture of certified, partially certified, certification expired, and uncertified systems. Testing to TADIL standards is a time-consuming process; the TADIL-J standards, for instance, take up 12 printed volumes. There is interest in finding ways to automate this testing

process. It would also be interesting to examine testing from a cost-benefit perspective: which standards are most or least important relative to their cost?

5.4 Joint Exercise Support

As part of its mission JITC provides interoperability support during the conduct of joint exercises throughout the world. In recent years these exercises have included Roving Sands, Joint Project Optic Cobra, ASCIET, and Ulchi Focus Lens. JITC's presence is valuable not only to the participants, but also to JITC itself. Joint exercises give JITC the opportunity to see how C4I systems are configured, perform, and fail in real-life situations. This knowledge allows JITC to refine its understanding of the interoperability requirements of the observed systems, and it promotes the design of better tests. Providing support at exercises also gives JITC the opportunity to learn about systems that have not been submitted for interoperability certification.

Currently, JITC makes use of information that it obtains from joint exercises by including summaries of its findings in quarterly Lessons Learned reports. Using this information more formally, as in an interoperability assessment, is problematical due to the structural disparity between joint exercises and operational tests.

The Institute for Joint Warfare Analysis (IJWA) at NPS studies joint exercises and analyzes data from them. IJWA has expressed a willingness to consider supporting research that finds commonality between the missions of IJWA and JITC.

6. NPS Educational Outreach

Both JITC government personnel and contractors expressed support for the idea of NPS faculty offering educational services to JITC. A relatively small number of JITC government personnel and contractors have Masters degrees, and only a few have Doctorates. Opportunities for taking advanced technical courses in the vicinity of Fort Huachuca or Sierra Vista, AZ are limited. Providing JITC with appropriately-structured educational products is another way that NPS can help JITC to perform its interoperability testing mission better.

An educational outreach program based on short courses and a remote teaching format may work best for JITC. Possible subjects include computer science, IT, M&S, probability and statistics, T&E, design of experiments, and electrical engineering.

List of Acronyms

AIS	automated information system
BMC4I	battle management C4I
BMDO	Ballistic Missile Defense Organization
C2	command and control
C3I	command, control, communications, and intelligence
C4I	command, control, communications and computers intelligence
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COE	Common Operating Environment
COP	Common Operational Picture
COTS	commercial, off-the-shelf
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DIT	Defense Information Testbed
DMS	Defense Messaging System
DMSO	Defense Modeling and Simulation Office
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	Department of Defense Intelligence Information System
DOT&E	Director, Operational Test & Evaluation
EKMS	Electronic Key Management System
FOM	Federated Object Module
FoS	family of systems
GCCS	Global Command and Control System
GCSS	Global Command Support System
GOTS	government, off-the-shelf
HLA	High Level Architecture
HWIL	hardware-in-the-loop
I&RTS	Integration & Run Time Specifications
IA	information assurance
IJWA	Institute for Joint Warfare Analysis
IO	information operations
IT	information technology
IW	information warfare
JCS	Joint Chiefs of Staff
JCTN	Joint Composite Tracking Network
JIES	Joint Interoperability Evaluation System
JITC	Joint Interoperability Test Command
JITF	Joint Integration Test Facility
JPN	Joint Planning Network
JTDL	Joint Tactical Data Link
JTF	Joint Test Facility

JTLS	Joint Theater Level Simulation
M&S	modeling and simulation
MDAP	Major Defense Acquisition Program
MNS	Mission Needs Statement
MOP	measure of performance
MOVES	Modeling, Visual Environments and Simulation
MRTFB	Major Range and Test Facility Base
NPS	Naval Postgraduate School
NSA	National Security Agency
ORD	Operational Requirements Document
OT&E	operational test and evaluation
OTH	over the horizon
PATRIOT	Phased Array Tracking Radar Intercept on Target
PKI	Public Key Infrastructure
RAM	reliability, availability, and maintainability
RTI	run-time interface
RTO	Responsible Test Organization
SCOPE	Systems Capable of Planned Expansion
SIPRNET	Secret Internet Protocol Router Network
SME	subject-matter expert
SWEG	Simulated Warfare Environment Generator
T&E	test and evaluation
TADIL	Tactical Digital Information Link
TEMP	Test and Evaluation Master Plan
THAAD	Theater High Altitude Area Defense
TMD	Theater Missile Defense
TS	Top Secret
TS/SCI	Top Secret/Sensitive Compartmented Information
VVA	verification, validation, and accreditation
Y2K	Year 2000

INITIAL DISTRIBUTION LIST

1. Research Office (Code 09) 1
 Naval Postgraduate School
 Monterey, CA 93943-5000

2. Dudley Knox Library (Code 013)..... 2
 Naval Postgraduate School
 Monterey, CA 93943-5002

3. Defense Technical Information Center 2
 8725 John J. Kingman Rd., STE 0944
 Ft. Belvoir, VA 22060-6218

4. Therese Bilodeau (Editorial Assistant) 1
 Dept of Operations Research
 Naval Postgraduate School
 Monterey, CA 93943-5000

5. Prof. Robert A. Koyak (Code OR/Kr) 18
 Dept of Operations Research
 Naval Postgraduate School
 Monterey, CA 93943-5000

6. RADM Raymond Smith 1
 Chief of Naval Operations (N81)
 Navy Department
 Washington, DC 20350

7. Prof. Peter Purdue, Dean..... 1
 Division of Operational and Applied Sciences
 Naval Postgraduate School
 Monterey, CA 93943-5001

8. Prof. Richard E. Rosenthal (Code OR), Chairman 1
 Operations Research Department
 Naval Postgraduate School
 Monterey, CA 93943-5000

9. Prof. Dan C. Boger (Code CS), Chairman 5
 Department of Computer Science
 Naval Postgraduate School
 Monterey, CA 93943-5000

10. Prof. Michael J. Zyda (Code CS/Zk) 2
 Department of Computer Science
 Naval Postgraduate School
 Monterey, CA 93943-5000

11. Prof. William Kemple 1
 Institute for Joint Warfare Analysis
 Naval Postgraduate School
 Monterey, CA 93943-5000

12. Prof. Gordon E. Schacher 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5000

13. Dr. Jeremy M. Kaplan, Deputy Director..... 1
C4I Modeling, Simulation and Assessment (D8) Staff
Defense Information Systems Agency
701 Courthouse Road
Arlington, VA 22204-2119

14. Col. Thomas L. Andrews, USAF, Commander 1
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

15. Mr. Denis Beaugureau, Deputy Commander..... 1
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

16. Mr. Randon Herrin, OT&E Test Director..... 4
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

17. Mr. Steve Bridges, Technical Director 1
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

18. Lt.Col. G.S. Brock, USMC, Chief..... 1
Warfighter Support Division
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

19. Mr. Mike Mangan, Chief..... 3
Automated Systems & Test Support Division
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

20. Mr. Leslie Claudio, Chief..... 1
Networks, Transmission & Integration Division
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020

21. Mr. Rick Meador, Chief..... 1
Operational Test & Evaluation Division
Joint Interoperability Test Command
Building 57305
Fort Huachuca, AZ 85613-7020